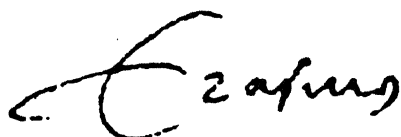


ECONOMETRIC INSTITUTE

A NEW PROOF OF CARTIER'S THIRD THEOREM

M. HAZEWINKEL

A handwritten signature in black ink, appearing to read 'Erasmus', is centered on the page.

REPORT 7810/M

ABSTRACT.

Let $\underline{\underline{Gf}}_A$ be the category of finite dimensional commutative formal groups over a ring A . To A one associates a certain, in general noncommutative, ring $\text{Cart}(A)$. One then defines a functor $G \rightarrow C(G)$ which assigns to a formal group law G its group of curves which is a module over $\text{Cart}(A)$. Theorems 2 and 3 of [1] now say that $G \rightarrow C(G)$ is an equivalence of categories of $\underline{\underline{Gf}}_A$ with a certain full subcategory of $\text{Cart}(A)$ -modules. In this paper we give a new proof of theorem 3 of [1], Cartier's third theorem, which asserts that every $\text{Cart}(A)$ -module of a certain type comes from a formal group law over A . This proof is based on the constructions of part IV of this series of papers [3].

Contents.

1. Introduction and statement of the theorem
2. Construction of a universal curve module
3. The universal ring L_C
4. Proof of Cartier's third theorem
5. The local case

March 25, 1978

Preliminary and Confidential

1. INTRODUCTION AND STATEMENT OF THE THEOREM.

From now on formal group means finite dimensional formal group law over A . We take the naive or power series point of view; i.e. an m -dimensional formal group over A is simply an m -tuple of power series $G(X,Y)$ in $2m$ variables $X_1, \dots, X_m; Y_1, \dots, Y_m$ such that $G(X,0) = X, G(0,Y) = Y, G(X,G(Y,Z)) = G(G(X,Y),Z), G(X,Y) = G(Y,X)$.

1.1. Curves. A curve (over A) in a formal group G over A is an m -tuple of power series $\gamma(t) = (\gamma_1(t), \dots, \gamma_m(t))$ in one variable t , such that $\gamma(0) = 0$. Two curves $\gamma(t), \delta(t)$ can be added by means of the formula $\gamma(t) +_G \delta(t) = G(\gamma(t), \delta(t))$. This turns the set of all curves into an abelian group $C(G)$. We use $C^n(G)$ to denote the subgroup of all curves $\gamma(t)$ such that $\gamma(t) \equiv 0 \pmod{t^n}, n = 1, 2, \dots$. This defines a filtration $C(G) = C^1(G) \supset C^2(G) \supset \dots$ and $C(G)$ is complete in the topology defined by this filtration.

1.2. The Operators. $\langle a \rangle, \underline{V}_n, \underline{f}_n$. In addition to the topological group structure on $C(G)$ one has a number of operators which are compatible with this structure. Viz.:

$$\begin{aligned} \text{for all } a \in A, \quad \langle a \rangle \gamma(t) &= \gamma(at) \\ \text{for all } n = 1, 2, \dots, \quad \underline{V}_n \gamma(t) &= \gamma(t^n) \end{aligned}$$

The definition of the third kind of operator, the Frobenius operators \underline{f}_n , needs a bit more care. Formally one has

$$\text{for all } n = 1, 2, \dots, \quad \underline{f}_n \gamma(t) = \gamma(\zeta_n t^{1/n}) +_G \dots +_G \gamma(\zeta_n^n t^{1/n})$$

where ζ_n is a primitive n -th root of unity. For a more precise definition cf. [3] part IV or [5]. There are various relations among these operators. They are

$$\begin{aligned} \langle a \rangle \langle b \rangle &= \langle ab \rangle, \quad \langle 1 \rangle = \underline{V}_1 = \underline{f}_1 = \text{identity operator}, \\ \underline{V}_m \underline{V}_n &= \underline{V}_{mn}, \quad \underline{f}_m \underline{f}_n = \underline{f}_{mn}, \\ \langle a \rangle \underline{V}_m &= \underline{V}_m \langle a^m \rangle, \quad \underline{f}_m \langle a \rangle = \langle a^m \rangle \underline{f}_m \\ (1.3) \quad \text{if } (n,m) &= 1, \text{ then } \underline{f}_m \underline{V}_n = \underline{V}_n \underline{f}_m, \\ \underline{f}_n \underline{V}_n &= n, \text{ i.e. } \underline{f}_n \underline{V}_n \gamma(t) = \gamma(t) +_G \gamma(t) +_G \dots +_G \gamma(t) \quad (n \text{ factors}), \\ \langle a+b \rangle &= \sum_{n=1} \underline{V}_n r_n(a,b) \underline{f}_n, \end{aligned}$$

where the $r_n(Z_1, Z_2)$ are the polynomials with coefficients in \mathbb{Z} defined by

$$(1.4) \quad r_n(Z_1, Z_2) = \sum_{d|n} dr_d(Z_1, Z_2)^{n/d}$$

1.5. A \mathbb{V} -basis for $C(G)$. Let $\delta_i(t)$ denote the curve $(0, \dots, 0, t, 0, \dots, 0)$ in G , where t is in the i -th spot. It immediately follows from $F(X, Y) \equiv X + Y \pmod{\text{degree } 2}$ that every curve in G can be uniquely written as a convergent sum

$$(1.6) \quad \gamma = \sum_{i=1}^n \sum_{k=1}^{\infty} \mathbb{V}_k \langle a_{ik} \rangle \delta_i$$

It follows, cf. (1.3) and also section 2 below, that we know the structure of $C(G)$ as a topological group with operators $\langle a \rangle$, $\mathbb{f}_n, \mathbb{V}_n$ if we know all the expressions

$$(1.7) \quad \mathbb{f}_n \delta_i = \sum_{s=1}^{\infty} \sum_{j=1}^m \mathbb{V}_s \langle c(n, s)_{ji} \rangle \delta_j$$

The "structure coefficients" $c(n, s)_{ji}$, $n, s \in \mathbb{N}$, $i, j \in \{1, \dots, m\}$ are far from independent. They satisfy certain relations which come from $\mathbb{f}_n \mathbb{f}_r = \mathbb{f}_{nr}$.

1.8. Reduced $\text{Cart}(A)$ -modules. If $C(G)$ is the module of curves of a formal group G , then $C(G)$ has the following properties

- (i) There are subgroups C^n , closed under the operators $\langle a \rangle$, \mathbb{V}_r ; C is complete in the topology defined by the C^n and C^n is the smallest closed subgroup of C which contains all the $\mathbb{V}_r C$ with $r \geq n$.
- (ii) The operators $\langle a \rangle$, \mathbb{f}_n , \mathbb{V}_n are all continuous and satisfy the relations (1.3).
- (iii) There are elements $\delta_1, \dots, \delta_m \in C$ such that every element $\gamma \in C$ can be uniquely written as a convergent sum

$$\gamma = \sum_{s=1}^{\infty} \sum_{j=1}^m \mathbb{V}_s \langle a_{js} \rangle \delta_j$$

In general we shall call a topological abelian group C with operators $\langle a \rangle$, $\mathbb{V}_n, \mathbb{f}_n$ such that (i), (ii), (iii) hold a reduced $\text{Cart}(A)$ -module. (Here $\text{Cart}(A)$ stands for the set of all formal expressions $\sum \mathbb{f}_i \langle a_{ij} \rangle \mathbb{V}_j$, with for every j only finitely many i such that $a_{ij} \neq 0$. These expressions can be added and multiplied by means of the calculation rules (1.3) to form a (topological) ring of operators, cf. [4]).

1.9. Cartier's third theorem. Let C be a reduced $\text{Cart}(A)$ -module with \underline{V} -basis $\delta_1, \dots, \delta_m$. There there exists an m -dimensional formal group law G over A such that $C(G) \simeq C$ as $\text{Cart}(A)$ -modules with δ_i corresponding to the i -th element $\delta_i(t)$ of the canonical \underline{V} -basis of $C(G)$ described in 1.5.

This is theorem 3 of [1]. Cartier never published his proofs of the theorems of [1]. Proofs can be found in [5]; these are outlined in [4]. In [2] there is a proof of Cartier's third theorem for the case that A is torsion free. This proof breaks down if A has additive torsion.

The remainder of this paper mainly concerns still another proof of Cartier's third theorem based on the constructions of the earlier parts of these series of papers. This proof also provides a link between these constructions and the "intertwined function pair" considerations of [2].

2. CONSTRUCTION OF A UNIVERSAL CURVE MODULE.

Choose $m \in \mathbb{N}$ and choose a set of elements $\delta_1, \dots, \delta_m$. Let \hat{L}_C be the ring $\hat{L}_C = \mathbb{Z}[C(n,r)_{i,j} \mid r \in \mathbb{N}, n \in \mathbb{N} \setminus \{1\}, i, j \in \{1, \dots, m\}]$ of polynomials in the indeterminates $C(n,r)_{i,j}$. For convenience we also introduce $C(1,1)_{i,j} = 0$ if $i \neq j$, $C(1,1)_{i,i} = 1$, $C(1,r)_{i,j} = 0$ for all $r \in \mathbb{N} \setminus \{1\}$, $i, j \in \{1, \dots, m\}$.

Now consider the set M of all formal expressions

$$(2.1) \quad \sum_{s=1}^{\infty} \sum_{j=1}^m \underline{V} \langle a_{s,j} \rangle \delta_j \quad a_{s,j} \in \hat{L}_C$$

We now introduce the defining relations

$$(2.2) \quad \underline{f}_n \delta_i = \sum_{s=1}^{\infty} \sum_{j=1}^m \underline{V} \langle C(n,s)_{ji} \rangle \delta_j$$

for all $n \in \mathbb{N}$. One can now use the calculation rules (1.3) with the exception of the rule $\underline{f}_n \underline{f}_r = \underline{f}_{nr}$, and the defining relations (2.2) to add expressions of the form (2.1) and to define \underline{f}_r of such an expression, $r \in \mathbb{N}$.

To do this we start by showing how to rewrite any sum of the form

$$(2.3) \quad \sum_{s=1}^{\infty} \sum_{j=1}^m \sum_t \underline{V} \langle a_{s,j,t} \rangle \delta_j \quad a_{s,j,t} \in \hat{L}_C$$

in the form (2.1). Here for each $s \in \mathbb{N}$, $j \in \{1, \dots, m\}$ the index t runs over some finite index set which may depend on s and j .

For each $n \in \mathbb{N}$, let $\lambda(n)$ be the number of prime factors of n , i.e. $\lambda(1) = 0$ and if $n = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$, p_i a prime number, $r_i \in \mathbb{N}$, then $\lambda(n) = r_1 + \dots + r_t$. One now proceeds as follows

$$\begin{aligned} \sum_{s,j,t} \prod_{s \in \mathbb{N}} \langle a_{s,j,t} \rangle^{\delta_j} &= \sum_{j,t} \langle a_{1,j,t} \rangle^{\delta_j} + \sum_{s \geq 2} \sum_{j,t} \prod_{s \in \mathbb{N}} \langle a_{s,j,t} \rangle^{\delta_j} \\ &= \sum_{j} \sum_{i=1}^{\infty} \prod_{i \in \mathbb{N}} \langle b_{i,j} \rangle^{\delta_j} + \sum_{s \geq 2} \sum_{j,t} \prod_{s \in \mathbb{N}} \langle a_{s,j,t} \rangle^{\delta_j} \end{aligned}$$

where $b_{i,j} = r_i(a_{1,j,1}, a_{1,j,2}, \dots)$ with r_1, r_2, \dots the polynomials in k variables defined by

$$(2.4) \quad Z_1^n + \dots + Z_k^n = \sum_{d|n} dr_d(Z_1, \dots, Z_k)^{n/d}, \quad n = 1, 2, \dots$$

(Cf. (1.4); of course k may depend on j). Now use (2.2) to rewrite (2.3) further as

$$\begin{aligned} &\sum_j \langle b_{1,j} \rangle^{\delta_j} + \sum_j \sum_{i \geq 2} \prod_{i \in \mathbb{N}} \langle b_{i,j} \rangle^{\delta_j} + \sum_{\ell, k} \sum_{\ell \in \mathbb{N}} \langle C(i, \ell)_{kj} \rangle^{\delta_k} \\ &+ \sum_{s \geq 2} \sum_{j,t} \prod_{s \in \mathbb{N}} \langle a_{s,j,t} \rangle^{\delta_j} = \sum_j \langle b_{1,j} \rangle^{\delta_j} \\ &+ \sum_{j,k} \sum_{i \geq 2} \sum_{\ell} \prod_{i \in \mathbb{N}} \langle b_{i,j}^{\ell} C(i, \ell)_{kj} \rangle^{\delta_k} + \sum_{s \geq 2} \sum_{j,t} \prod_{s \in \mathbb{N}} \langle a_{s,j,t} \rangle^{\delta_j} \\ &= \sum_j \langle b_{1,j} \rangle^{\delta_j} + \sum_{\lambda(s) \geq 1} \sum_j \sum_t \prod_{s \in \mathbb{N}} \langle b'_{s,j,t} \rangle^{\delta_j} \end{aligned}$$

for certain well determined $b'_{s,j,t} \in \tilde{L}_C$. And of course the summation set for t for a given s, j will now in general be different than the one in (2.3). For each $s \in \mathbb{N}$ with $\lambda(s) \geq 1$ (i.e. $s \geq 2$) write $s = p_s s'$ where p_s is the first prime number dividing s . We find an expression

$$(2.5) \quad \sum_j \langle b_{1,j} \rangle^{\delta_j} + \sum_{\lambda(r)=1} \prod_{r \in \mathbb{N}} \left(\sum_{s,j,t} \prod_{s \in \mathbb{N}} \langle a'_{r,s,j,t} \rangle^{\delta_j} \right)$$

where now the summation set for t may also depend on r . Now repeat the

procedure given above for each of the interior sums

$$\sum_{s,j,t} \underline{v}_s \langle a'_{r,s,j,t} \rangle \delta_j$$

to obtain an expression

$$\sum_j \langle b_{1,j} \rangle \delta_j + \sum_{\lambda(r)=1} \underline{v}_r \sum_j \langle b_{r,1,j} \rangle \delta_j + \sum_{\lambda(r)=2} \underline{v}_r \sum_{s,j,t} \underline{v}_s \langle a''_{r,s,j,t} \rangle \delta_j$$

Now apply the same procedure to the interior sums in the third summand, ..., etc., ... After k steps we thus obtain algorithmically the coefficients $x_{s,j}$ in

$$(2.6.) \quad \sum_{s,j,t} \underline{v}_s \langle a_{s,j,t} \rangle \delta_j = \sum_{s,j} \underline{v}_s \langle x_{s,j} \rangle \delta_j$$

for all s with $\lambda(s) \leq k-1$.

We now proceed to define f_n of an expression (2.1). Write

$$(2.7) \quad \begin{aligned} f_n \left(\sum_{s,j} \underline{v}_s \langle a_{s,j} \rangle \delta_j \right) &= \sum_{s,j} \frac{d\underline{v}_s}{d\underline{n}/d} f_n \langle a_{s,j} \rangle \delta_j \\ &= \sum_{s,j} \frac{d\underline{v}_s}{d\underline{n}/d} \langle a_{s,j}^{n/d} \rangle_{f_n/d} \delta_j \\ &= \sum_{s,j,r,k} \frac{d\underline{v}_s}{d\underline{n}/d} \langle a_{s,j}^{n/d} \rangle_{\underline{v}_r} \langle C(n/d,r)_{k,j} \rangle \delta_k \\ &= \sum_{s,j,r,k} \frac{d\underline{v}_s}{d\underline{n}/d} \langle a_{s,j}^{nr/d} \rangle_{C(n/d,r)} \delta_k \end{aligned}$$

where $d = (s,n)$. This is a sum of the type (2.3), which then is put into the form (2.1) by the algorithmic procedure outlined above.

To complete this picture we also define

$$\begin{aligned} \underline{v}_r \left(\sum_{s,j} \underline{v}_s \langle a_{s,j} \rangle \delta_j \right) &= \sum_{s,j} \underline{v}_{rs} \langle a_{s,j} \rangle \delta_j \\ \langle \mathfrak{a} \left(\sum_{s,j} \underline{v}_s \langle a_{s,j} \rangle \delta_j \right) &= \sum_{s,j} \underline{v}_s \langle a^s_{s,j} \rangle \delta_j \end{aligned}$$

We have now defined a topological abelian group M with operators $\langle \mathfrak{a} \rangle$, \underline{v}_n , f_n for all $a \in \check{L}_C$, $n \in \mathbf{N}$. (The topology is the obvious one). Note that M is definitely not a $\text{Cart}(\check{L}_C)$ module. For one thing it is not at

all clear that \underline{f}_n is additive and obviously $\underline{f}_{n+m} = \underline{f}_{nm}$ does not hold in general. Before discussing the relations one must introduce to make a variant of M a $\text{Cart}(L_C)$ module over some quotient ring L_C of \hat{L}_C we note a homogeneity property. First make \hat{L}_C into a graded ring by giving $C(n,r)_{i,j}$ degree $nr - 1$ for all $n,r \in \mathbb{N}$, $i,j \in \{1, \dots, m\}$. We then have

2.8. Lemma. Suppose that in the sum (2.3) each $a_{s,j,t}$ is homogeneous of degree $ks - 1$ for some $k \in \mathbb{N}$ independent of s,j,t . Then the $x_{s,j}$ in (2.6) are homogeneous of degree $ks - 1$.

Proof. To prove this by induction it suffices to show that under the hypothesis stated the $b_{1,j}$ and $a'_{r,s,j,t}$ of (2.5) are respectively of degree $k - 1$ and $krs - 1$ respectively. Now $b_{1,j} = a_{1,j,1} + a_{1,j,2} + \dots$ which is homogeneous of degree $k - 1$. As to the $a'_{r,s,j,t}$, they are of two types, viz. 1^o) $a'_{r,s,j,t} = a_{rs,j,t}$ which by hypothesis is homogeneous of degree $krs - 1$, and 2^o) $a'_{r,s,j,t} = b_{i,j} C(i,\ell)_{k,j}$, with $i\ell = rs$. Now from (2.4) we see that $r_i(Z_1, \dots, Z_k)$ is homogeneous of degree i (if each Z_i is given degree 1) so that $b_{i,j} = r_i(a_{1,j,1}, a_{1,j,2}, \dots)$ is homogeneous of degree $i(k-1)$. It follows that $a'_{r,s,j,t} = b_{i,j}^\ell C(i,\ell)_{k,j}$ is homogeneous of degree $li(k-1) + i\ell - 1 = lik - 1 = krs - 1$. This proves the lemma.

2.9. Corollary. Let $\underline{f}_{n=\ell} \delta_i = \underline{f}_n (\sum_{s,j} \underline{v}_{s,j} \langle C(\ell,s)_{j,i} \rangle \delta_j) = \sum_{s,j} \underline{v}_{s,j} \langle y_{n,\ell,s,j,i} \rangle \delta_j$ where the $y_{n,\ell,s,j,i}$ are calculated as in (2.7). Then $y_{n,\ell,s,j,i}$ is homogeneous of degree $n\ell s - 1$.

Proof. In this particular case of (2.7) we have $a_{s,j} = C(\ell,s)_{j,i}$. Thus $a_{s,j}^{nr/d} C(n/d,r)_{k,j}$ is homogeneous of degree $d^{-1}nr(\ell s - 1) + d^{-1}nr - 1 = d^{-1}nr\ell s - 1 = (d^{-1}rs)n\ell - 1$ and the corollary follows by lemma 2.8.

2.10. Lemma. If $\ell > 1$ then $y_{n,\ell,t,i,j} \equiv nC(\ell,nt)_{i,j} \pmod{\text{(decomposables)}}$ (Here (decomposables) stands for the ideal of \hat{L}_C generated by all products of the form $C(n,r)_{i,j} C(s,t)_{k,\ell}$ with $n,s \in \mathbb{N} \setminus \{1\}$, $r,t \in \mathbb{N}$, $i,j,k,\ell \in \{1, \dots, m\}$).

Proof. From (2.7) we have

$$\sum_{t,j} \underline{v}_t \langle y_{n,\ell,t,j,i} \rangle \delta_j = \sum_{s,r,j,k} \underline{v}_{rs/d} \langle C(\ell,s)_{j,i}^{nr/d} C(n/d,r)_{k,j} \rangle \delta_k$$

where $d = (s, n)$ in the sum on the right. Choose a fixed $t \in \mathbb{N}$. By the rewriting procedure discussed in the beginning of this section a summand in the sum on the right can contribute to $y_{n, \ell, t, j, i}$ iff $d^{-1}rs \leq t$. Moreover, if this contribution is to be nonzero modulo decomposables we must in addition have $d = nr$, $d^{-1}n = 1$, $r = 1$, $k = j$ (because $\ell > 1$). It follows that s is a multiple of n and $s \leq tn$ so that the only contributions to $y_{n, \ell, t, j, i}$, which are possibly nonzero modulo decomposables, come from

$$\sum_{a=1}^t \sum_a n \langle C(\ell, an)_{j, i} \rangle \delta_j$$

However $n \langle C(\ell, an)_{j, i} \rangle = \langle nC(\ell, an)_{j, i} \rangle +$ (terms which are zero modulo decomposables). The lemma follows.

2.11 Remark. By definition one has $y_{1, n, s, j, i} = y_{n, 1, s, j, i} = C(n, s)_{j, i}$ so that lemma 2.10 does not hold for $\ell = 1$.

3. THE UNIVERSAL RING L_C .

Let L_C be the quotient ring of \tilde{L}_C obtained by factoring out the ideal generated by the homogeneous polynomials

$$(3.1) \quad C(n\ell, t)_{ji} - y_{n, \ell, t, j, i}, \quad n, \ell, t \in \mathbb{N}, \quad i, j \in \{1, \dots, m\}$$

3.2. Theorem. $L_C \cong \mathbb{Z} [T(n)_{i, j} \mid n = 2, 3, \dots; i, j \in \{1, \dots, m\}]$ as a graded ring, with degree $(T(n)_{i, j}) = n - 1$.

Proof. The ring L_C is graded because the polynomials (3.1) are homogeneous by corollary 2.8. Let $L_C^{(t)}$ be its homogeneous summand of degree $t - 1$ and let $M^{(t)}$ be the submodule of $L_C^{(t)}$ generated by the decomposables. Then $L_C^{(t)}/M^{(t)}$ is generated (as an abelian group) by the $C(s, r)$ with $sr = t$. Now by lemma 2.10 and the defining relations (cf. (3.1)) we see that modulo decomposables

$$C(rs, t)_{i, j} \equiv rC(s, rt)_{i, j}$$

for all $i, j \in \{1, \dots, m\}$, $s \in \mathbb{N} \setminus \{1\}$, $r \in \mathbb{N}$. It follows that if s is not a prime number, $s \neq 1$, and p is a prime number dividing s , then

$$(3.3) \quad C(s, r)_{i, j} \equiv p^{-1} s C(p, p^{-1} sr)_{i, j}$$

It readily follows that $L_C^{(t)}/M^{(t)}$ is the abelian group generated by the $C(p, p^{-1}t)_{i,j}$, where p runs through all prime divisors of t , subject to the relations

$$(3.4) \quad qC(p, p^{-1}t)_{i,j} \equiv pC(q, q^{-1}t)_{i,j}$$

for all prime number divisors p and q of t . If t is a power of a prime number p , $t = p^r$, this means that $L_C^{(t)}/M^{(t)}$ is a free abelian group of rank m^2 generated by the classes of the $T(t)_{i,j} = C(p, p^{-1}t)_{i,j}$. If t is not a power of a prime number let $P(t)$ be the set of prime numbers dividing t . Choose $\mu(p) \in \mathbb{Z}$ such that

$$(3.5) \quad \sum_{p \in P(t)} p\mu(p) = 1$$

Let

$$T(t)_{i,j} = \sum_{p \in P(t)} \mu(p)C(p, p^{-1}t)_{i,j}$$

It then follows from (3.3) and (3.4) that $L_C^{(t)}/M^{(t)}$ is the free abelian group of rank m^2 generated by the classes of the $T(t)_{i,j}$. This proves the theorem.

3.6. Remark. (Construction of a "universal $\text{Cart}(L_C)$ -module" (continued))

Let C_C be the set of all expressions $\sum_{s,j} \underline{v}_s \langle a_{s,j} \rangle \delta_j$ with $a_{s,j} \in L_C$. Now

calculate sums and $\underline{f}_r \gamma$, $\langle a \rangle \gamma$, $\underline{v}_r \gamma$ for $\gamma \in C_C$ as in section 2. Then C_C is in fact a $\text{Cart}(L_C)$ module. One has of course $\underline{f}_n \underline{f}_\ell \delta_i = \underline{f}_{n\ell} \delta_i$ by the relations defining L_C . And, using this, one can now prove directly that the $\langle a \rangle$, \underline{f}_n , \underline{v}_n are additive and that all the relations (1.3) hold. This also follows from the isomorphism result below, cf. remark 4.7.

4. PROOF OF CARTIER'S THIRD THEOREM.

Let $F(X,Y)$ be any m -dimensional formal group law over a ring A . Let $\delta_1(t), \dots, \delta_m(t)$ be the standard \underline{v} -basis for $C(F)$. Then we have unique expressions, cf. (1.7),

$$\underline{f}_n \delta_i(t) = \sum_{s=1}^{\infty} \sum_{j=1}^m \underline{v}_s \langle c(n,s)_{j,i} \rangle \gamma_j(t)$$

Now define $\tilde{\eta}: \hat{L}_C \rightarrow A$ by $\tilde{\eta}(C(n,s)_{i,j}) = c(n,s)_{i,j}$.

Because $\underline{f}_{n=\ell} \gamma_i(t) = \underline{f}_{n\ell} \gamma_i(t)$ in $C(F)$ for all m, ℓ, i it follows that

$$\tilde{\eta}(y_{n,\ell,s,j,i}) = c(n\ell,s)_{j,i}$$

for all $s, \ell, n \in \mathbb{N}$, $i, j \in \{1, \dots, m\}$. Therefore $\tilde{\eta}$ induces a homomorphism of rings $\eta_F: L_C \rightarrow A$. We can in particular apply this to the case $F(X, Y) = F_R(X, Y)$, the universal curvilinear m -dimensional formal group law over $\mathbb{Z}[R] = \mathbb{Z}[R_n(i, j) \mid n \in \mathbb{N} \setminus \{1\}, i, j \in \{1, \dots, m\}]$ of [3], part IV. This gives us a homomorphism.

$$(4.1) \quad \eta_C: L_C \rightarrow \mathbb{Z}[R]$$

4.2. Theorem. The homomorphism η_C of (4.1) is an isomorphism of graded rings.

Proof. Let $f_R(X)$, the logarithm of $F_R(X, Y)$, be equal to $f_R(X) = \sum_{n=1}^{\infty} b_n(R) X^n$.

Recall that

$$(4.3) \quad b_n(R) = \sum_{(i_1, \dots, i_s)} d(i_1, \dots, i_s) R_{i_1}^{(i_1)} R_{i_2}^{(i_1 \dots i_{s-1})} \dots R_{i_s}^{(i_1 \dots i_{s-1})},$$

$$b_1(R) = I_m$$

where R_k is the matrix $(R_k(j, \ell))_{j, \ell}$ and the sum is over all sequences (i_1, \dots, i_s) , $i_j \in \mathbb{N} \setminus \{1\}$, $s \geq 1$, $i_1 i_2 \dots i_s = n$. Here the $d(i_1, \dots, i_s)$ are certain well-determined coefficients, and $R_i^{(j)}$ is the matrix obtained from R_i by raising each of its entries to the power j . Cf. [3], part IV, section 2. Then $b_n(R)$ is homogeneous of degree $n - 1$ if $R_k(j, \ell)$ is given degree $k - 1$. Let $\delta_1(t), \dots, \delta_m(t)$ be the standard \underline{V} -basis for $C(F_R)$ and let

$$(4.4) \quad \underline{f}_p \delta_i(t) = \sum_{s, j} \underline{V}_s \langle c(p, s)_{j, i} \rangle \delta_j(t)$$

Now $\underline{f}_R(\gamma(t) + \underline{F}_R \delta(t)) = \underline{f}_R(\gamma(t)) + \underline{f}_R(\delta(t))$ (ordinary coefficientwise

sum), by the definition of logarithm. It follows that $\underline{f}_R(\underline{f}_p \gamma(t)) = \sum_{i=1}^{\infty} p z_{pi} t^i$

if $f_R(\gamma(t)) = \sum z_i t^i$, $z_i \in \mathbb{Q}[R]^m$. Applying f_R to (4.4) it follows that

$$(4.5) \quad p b_{pn}(R) = \sum_{d|n} b_{n/d}(R) c(p,d)^{n/d}$$

(This formula provides the link with the "intertwined function pair" considerations of [2]).

With induction it follows from (4.5) that the $c(p,s) \in \mathbb{Z}[R]$ are homogeneous of degree $ps - 1$ (, that is to say the entries of these $m \times m$ matrices are homogeneous of degree $ps-1$). Now $b_{pn}(R) \equiv p^{-1} R_{pn}$ modulo decomposables if n is a power of p and $b_{pn}(R) \equiv R_{pn}$ modulo decomposables if n is not a power of a prime number, cf (4.3) and use that $d(i_1) = p^{-1}$ if i_1 is a power of a prime number p and $d(i_1) = 1$ if i_1 is not a power of a prime number, cf. [3], part IV, section 2.

It follows that η_C satisfies

$$\eta_C(C(p, p^{r-1})_{i,j}) \equiv R_p(i,j) \pmod{\text{decomposables}}$$

$$\eta_C(C(p,s)_{i,j}) \equiv pR_{ps}(i,j) \pmod{\text{decomposables}}$$

if s is not a power of p . Hence $\eta_C(T_p(i,j)) \equiv R_p(i,j) \pmod{\text{decomposables}}$,

and if s is not a power of a prime number

$$\eta_C(T_s(i,j)) = \eta_C\left(\sum_{p \in P(s)} \mu(p) C(p, p^{-1}s)_{i,j}\right) \equiv \sum_{p \in P(s)} \mu(p) pR_s(i,j) = R_s(i,j)$$

modulo(decomposables). Here $P(s)$ and the $\mu(p)$ are as in (3.5). It follows that η_C is indeed an isomorphism (homogeneous of degree zero).

4.6. Proof of Cartier's third theorem. Let C be a reduced $\text{Cart}(A)$ module, i.e. C is a topological abelian group such that the properties of 1.8 hold. Let $\delta_1, \dots, \delta_m$ be a \mathbb{Y} -basis for C . Then every $\sum_n \delta_i$ can be uniquely written as a convergent sum (cf. (1.7)),

$$\sum_n \delta_i = \sum_{s=1}^{\infty} \sum_{j=1}^m \sum_s \langle c(n,s)_{j,i} \rangle \delta_j \quad c(n,s)_{j,i} \in A$$

Now define $\tilde{\eta}: \tilde{L}_C \rightarrow A$ by $\tilde{\eta}(C(n,s)_{j,i}) = c(n,s)_{j,i}$. Because $\sum_n f_\ell = \sum_n f_\ell$

in C we have that

$$\tilde{\eta}(C(n\ell, s)_{j,i}) = \tilde{\eta}(y_{n,\ell,s,j,i})$$

for all n, ℓ, s, j, i so that $\tilde{\eta}$ factorizes through L_C to define a homomorphism $\eta: L_C \rightarrow A$. Now let $\phi: \mathbb{Z}[R] \rightarrow A$ be equal to $\phi = \eta\eta_C^{-1}$, where η_C is the isomorphism of theorem 4.2. Then $F(X, Y) = \phi_* F_R(X, Y)$ is a formal group law over A such that $C(F) \simeq C$ as a topological group with operators. The isomorphism is given by $\delta_i(t) \rightarrow \delta_i$, where $\delta_1(t), \dots, \delta_m(t)$ is the standard \underline{V} -basis of $C(F)$.

4.7. Remark. The module C_C of 3.6 above is the module of curves of the formal group law $(\eta_C^{-1})_* F_R(X, Y)$ over L_C .

5. THE LOCAL CASE.

Choose a prime number p and suppose that A is a $\mathbb{Z}_{(p)}$ -algebra. Then the formal groups G over A can be classified by a much smaller group of curves $C_p(G) \subset C(G)$, with a much simpler ring of operators. In detail $C_p(G) = \{\gamma(t) \in C(G) \mid \underline{f}_q \gamma(t) = 0 \text{ for all prime numbers } q \neq p\}$. The operators on $C_p(G)$ are the $\underline{V}_p^i, \underline{f}_p^i$ and $\langle a \rangle, a \in A, i \in \mathbb{N} \cup \{0\}$. The topological group of p -typical curves $C(G)$ has filtration subgroups $C_p^{(n)}(G) = C_p(G) \cap C^{p^n}(G)$ and is complete in the topology defined by this filtration. One shows that the topological groups with operators thus obtained satisfy

(i) $C_p(G)$ is a complete Hausdorff topological group with operators $\underline{V}_p^i, \underline{f}_p^i, \langle a \rangle$ which satisfy analogous relations (1.3) obtained by setting $\underline{V}_n = 0 = \underline{f}_k$ for all $k, n \in \mathbb{N}$ which are not a power of p .

(ii) The topology of $C_p(G)$ is defined by the subgroups $C_p^{(n)}(G) = \underline{V}_p^n C(G)$

(iii) There are elements $\delta_i(t), i = 1, \dots, m \in C_p(G)$ such that every curve $\gamma(t) \in C_p(G)$ can be written as a unique convergent sum

$$\gamma = \sum_{n=0}^{\infty} \sum_{j=1}^m \underline{V}_p^{n \langle a_{n,i} \rangle} \delta_i$$

(To prove (iii) one uses Corollary (2.11) of [3] part IV to reduce to the case that G is a p -typical formal group and in that case the standard basis curves $\delta_i(t) = (0, \dots, 0, t, 0, \dots, 0)$ are p -typical and satisfy (iii)).

Inversely, the local version of Cartiers third theorem says that every filtered topological group $C \supset C^1 \supset C^2 \supset \dots$ with operators $\underline{V}_p, \underline{f}_p, \langle a \rangle$ such that (i), (ii), and (iii) hold comes from a formal group over A .

The proof of this is a triviality, given the construction of the m -dimensional p -typical universal formal group $F_V(X,Y)$ of [3], part IV. Let $\delta_i(t)$ be the i -th standard curve over $\mathbb{Z}[V] = \mathbb{Z}[V_n(i,j) | n \in \mathbb{N}, i, j, \in \{1, \dots, m\}]$ in $C(F_V)$. Then one calculates as in section 4 above

$$(5.1) \quad \mathbb{f}_p \delta_i(t) = \sum_{n=0}^{\infty} \sum_{j=1}^m \mathbb{V}_p^n \langle V_{n+1}(j,i) \rangle \delta_j(t)$$

where one uses that the logarithm $f_V(X)$ of $F_V(X,Y)$ satisfies

$$f_V(X) = \sum_{n=0}^{\infty} a_n(V) X^{p^n}$$

$$p a_n(V) = a_{n-1}(V) \mathbb{V}_1^{(p^{n-1})} + \dots + a_1(V) \mathbb{V}_{n-1}^{(p)} + \mathbb{V}_n$$

cf. [3], parts II and IV

Now let C be any topological group with operators $\mathbb{f}_p, \mathbb{V}_p, \langle a \rangle, a \in A$ such that (i) - (iii) hold. Choose $\delta_1, \dots, \delta_m$ such that (iii) holds and let

$$(5.2) \quad \mathbb{f}_p \delta_i = \sum_{n=0}^{\infty} \sum_{j=1}^m \mathbb{V}_p^n \langle a_{n,j,i} \rangle \delta_j$$

Define $\phi: \mathbb{Z}[V] \rightarrow A$ by $\phi(V_{n+1}(j,i)) = a_{n,j,i}$. Then $\phi_* F_V(X,Y)$ is a formal group law over A such that $C_p(\phi_* F_V) \simeq C$ as topological groups with operators. The isomorphism is given by $\delta_i(t) \mapsto \delta_i$, where $\delta_i(t)$ is the curve $(0, \dots, 0, t, 0, \dots, 0)$ in $C_p(\phi_* F_V)$. This follows from (5.2) as compared to (5.1).

REFERENCES.

1. P. Cartier, Modules associés à un groupe formel commutatif. Courbes typiques, C.R. Acad. Sci. Paris 265(1967), A 129-132.
2. E. Ditters, Cours de groupes formels, Lect. Notes, Orsay, 1975
3. M. Hazewinkel, Constructing Formal Groups I - VIII, I: J. Pure and Applied Algebra 9(1977), 131-150; II: *ibid* 9(1977), 151-162; III: *ibid.* 10(1977), 1 - 18 ; IV-VII: Adv. Math., to appear; VIII: Compositio Math., submitted.
4. M. Lazard, Sur les théorèmes fondamentaux des groupes formels commutatifs, Indagationes Math. 35, 4 (1973), 281-300, Errata et Addenda, *ibid* 36, 2 (1974), 122-124.
5. M. Lazard, Commutative Formal Groups, Springer, 1975, Lect. Notes Math. 443.